IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Massimiliano Antonio Poletto et al.	Art Unit	: 2184
		Examiner	: Perungavoor, Venkatanaray
Serial No.	: 10/066,232	Conf. No.	: 2754
Filed	: January 31, 2002		
Title	: DENIAL OF SERVICE ATTACKS CHARACTERIZATION		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Pursuant to 37 C.F.R. § 41.41, Applicant responds to the Examiner's Answer as follows

Rejection of Claims 7, 9-14, 19-23, and 26 over Botros.

Claims 7, 19, 20, 21 and 26

The examiner maintains the rejection of these claims arguing now that:

> **As Botros discloses the producing of an histogram of received network traffic see Col 3 Ln 37-51 & Fig. 10 & Fig. 11. The network traffic disclosed by Botros includes the user activities and peer activities collectively being stored on a data store for comparison to detect abnormal behavior thorough the use of a histogram see Col 4 Ln 17-25. Where the network is being examined initially to collect data on the users on the network and form a distribution of users, i.e. histogram see Col 3 Ln 37-44. Botros discloses the raw data collected include the data of commands performed, user activities see Col 6 Ln 53-62....** [1]

The examiner seems to equate "user activities" with network traffic and indeed Botros may use a network to collect data on "user activities." Indeed, in the examiner's explanation, the examiner further goes on to state that:

> **Botros mentions the user activity being divided into more categories to collect data for building a histogram including monitoring of file access, resource usage, login failures, whereby the listing suggests network traffic see Col 7 Ln 11-23. In that, resource and files are most likely shared on a network through a server and monitoring of these characteristics suggests a monitoring of network traffic."** [2]

[1] Examiner's Answer page 9
[2] Id.

However, claim 7 requires: "producing a histogram of received network traffic for at least one parameter of network packets and characterizing an attack based on comparison of a historical histogram with the produced histogram data for one or more parameters." Thus, the histogram is of network traffic but at the level of the network packets and for a parameter of the network packets, as explicitly recited. Botros does not disclose any mechanism to collect data on a parameter of network packets, construct a histogram of that parameter and compare that histogram to a historical histogram for that parameter or indeed disclose network packets or network traffic.

Accordingly Botros cannot anticipate claim 7, nor render claim 7 obvious, since Botros does not possess of all elements of the claimed invention arranged as in the claim. See *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983).

Claims 9 and 10

The examiner argues that: "As Botros discloses the time periods being varied from 4 to 6 months see Col 10 Ln 29-39." However, claim 9 for instance requires that: "the historical histogram is based on time periods that can range from 1 hour to 1 week or more." There is no description in Botros of time periods having the duration as in claim 9.

Claims 11-14

The examiner continues to argue that: "Botros discloses the computation of the difference in the historical and produced histograms see Col 9 Ln 39-44." Appellant contends that no such teaching is present in Botros. Botros merely describes that:

> **This is done by subtracting the user's current activity value from the peer historical mean and dividing the result by the peer historical standard deviation. This deviation or anomalous behavior is translated into a numerical value and added to the features list 106 at step 708.**

This is not understood to describe the claimed of features of: "normalizing the produced and the historical histograms for each parameter and computing their difference to identify

significant outliers that are considered indicators of suspicious traffic," as recited in claim 11. There is no mention in Botros that the histograms are used in subtracting.

Claims 19, 20, and 26

Appellant contends that Botros does not describe the data collectors as used in claims 19, 20 and 26. The examiner equates the function of a database to that of a data collector. However, the function of the data collector is to collect statistical information, as described by Appellant, and specifically, as claimed by Appellant in claim 19, to execute the method on the data collector. Botros "database" is not described as capable of executing any method that would correspond to that recited in claim 7.

Claims 22 and 23

Regarding Appellant's claim 22 the examiner argues: "... Botros discloses the setting of probabilistic parameters accurately to reduce "false positive" and not to be desensitive (sic) to intrusions see Col 12 Ln 52- Col 13 Ln 3. Where the factor is being adjusted to capture the intrusions and to avoid false alerts, thereby reducing blocking legitimate traffic."

Claim 22 however deals with correlation of suspicious parameters to reduce blocking of legitimate traffic. Botros on the other hand does not describe any correlation process. Moreover, the examiner's reliance on Botros is directed to training of a neural network model of Botros, not to any correlation of suspicious parameters to reduce blocking of legitimate traffic.

Rejection of Claims 1-6, 8, 15-18, 24-25, 27, 30-36 over Botros in view of Wetherall

Claims 1, 3 and 4

The examiner does not use Wetherall to teach a parameter of network traffic and does not address the distinction between the language of claim 7 and claim 1, namely that claim 7 explicitly mentions network packets as the source of the network traffic. Claim 1, in contrast, does not mention packets explicitly but instead uses a short-hand expression of "network traffic."

However, even with respect to the arguments made by the examiner in claim 7, where the examiner ignored the fact that claim 7 explicitly mentions network packets, the examiner has not shown that Botros describes or suggests: "a detection process to determine if the values of a parameter of network traffic exceed normal values for the parameter to indicate an attack on the data center."

The examiner also maintains that Botros teaches: "exceeding of normal values ... in the same terms as the instant invention see Col 9 Ln 31-46." However, there Botros merely mentions calculation of activities for a selected user. There is no teaching of "a parameter of network traffic exceed[s] normal values for the parameter to indicate an attack on the data center." Botros is merely dealing with user activities not a parameter of network traffic.

Appellant's however also notes that the histograms described by Botros are used to train models not to compute significant outliers and classifying an attack, as claimed.

The examiner argues that: "At the outset, the Appellant has misunderstood the rejection. The error on part of the Examiner was to say that Botros does not disclose the parameters to compute significant outliers and classify attacks." Appellant asks: "How can the examiner state that Appellant has misunderstood the rejection, when the examiner readily admits that the examiner erred in presenting the rejection, failing therefore to afford Appellant an opportunity to argue and/or amend the claims to overcome the rejection?"

Nonetheless, the examiner was previously correct, in that Botros as argued above and of record, does not disclose the parameters to compute significant outliers and classify attacks. Accordingly, the examiner is left with the teachings of Wetherall but like Botros Wetherall also does not disclose the filtering packets based on characterization, as recited in claim 1.

The examiner argues that:

> **The Appellant's argument regarding the modifying of Botros with Wetherall would not serve any purpose of Botros is not persuasive. As Botros deals with generation of histograms and comparing of historical histograms for attack. Similarly, Wetherall deals with generation of histograms and comparing of historical histograms to classify attacks, further advancing Botros by the inclusion of filters serving to eliminate spoofed addresses. Thus, both pieces of prior art are relevant to the instant invention and both disclose to an great detail the instant invention.**

Appellant contends that there exists no suggestion to combine Botros with Wetherall for all of the reasons of record. Moreover, the examiner's newly stated motivation quoted above only serves to undercut the previous argument made by the examiner, namely that: "Wetherall deals with generation of histograms and comparing of historical histograms to classify attacks, further advancing Botros by the inclusion of filters serving to eliminate spoofed addresses." However, this would be tantamount to modifying Botros to include features not even contemplated by Botros, since nowhere does Botros discuss spoofing attacks, spoofed address, or indeed network packets or network traffic.

Accordingly, neither Botros nor Wetherall taken together or separately suggest a detection process to determine if the values of a parameter of network traffic exceed normal values for the parameter to indicate an attack on the data center, a characterization process to build a histogram for the parameter to compute significant outliers in a parameter and classify the attack and a filtering process for filtering of network packets based on the characterization process.

Claims 2 and 5

Appellant's claim 2 specifically deals with representing suspicious parameter values by a bit vector to track good and bad values. Botros neither describes nor suggests a bit vector. Moreover, contrary to the examiner's interpretation of Botros, Botros disclosure of: "the ratio containing a mixture of bad and good values see Col 12 Ln 37-39." is again directed to training a model and selecting values that have a mixture of bad and good. These teachings have no relevance to the characterization process that represents suspicious parameter values by a bit vector with a 1 in every position corresponding to a "bad" value, and a 0 in every position corresponding to a "good" value.

The examiner argument that Wetherall's "profile," which the examiner characterizes as a "bit vector", "broadly speaking" is completely without merit. The examiner argues that because data embodied within a computer "consists of bits, is being used as a reference for future

comparison to detect attacks." However, that is not a bit vector and indeed is an illogical and improper argument.

Claim 6

The examiner argues that because "... Wetherall discloses the source address being used to gather data for generation of a histogram and further of the histogram being used to compare the historical histogram further filtering of packets see Par. 0012. Wetherall at least suggests claim 6." Appellant disagrees. While claim 6 mentions source address, claim 6 uses the source address to determine if the values of source address exceed normal values to indicate an attack. Wetherall, in contrast does not classify the attack based on the source IP Address, but instead uses a histogram of source address as a basis for filtering of the packets.

Claim 8

The Examiner refers the board to the examiner's argument in Claims 2 and 5.

Claims 15-17

The now argues that Wetherall discloses that the reference profile being used to compare with current profile see Par, 0056 corresponds to the master correlation bit vector, advancing the reasoning that: "And this is done through the use of digitalizing the data, i.e. bit vector, and further comparing thorough viewing resemblance to the reference profile, bit vector, see Par. 0036-0037. And further, the reference profile is constant-time, independent of other profiles see Par. 0040." For all of the reasons discussed above for the bit vector this line of reasoning that these functions occur in a computer using digitized data are totally without merit.

Claim 18

The Examiner refers the board to the examiner's argument in Claim 6.

Claim 25

The Examiner refers the board to the examiner's argument in Claims 1, 3 and 4 above.

Claims 32, 35 and 36

The examiner states that: "Appellant's only argument appears to be that filtering using histogram to characterize attacks is not being disclosed by Wetherall. ... "

Appellant contends that this is incorrect. Appellant clearly argued that the features of claim 32 included monitoring network traffic through a gateway disposed between the data center and a network, determining if values of at least one parameter exceed normal, threshold values expected for the parameter to indicate an attack on the site, producing a histogram for the at least one parameter of network traffic to characterize the attack by comparing the histogram to at least one historical histogram for that parameter, and filtering out traffic based on characterizing the traffic, which the gateway deems to be part of an attack.

The focus on filtering simply addressed the focus of the examiner's rejection. However no combination of Botros with Wetherall suggests: monitoring network traffic through a gateway disposed between the data center and a network, determining if values of at least one parameter exceed normal, threshold values expected for the parameter to indicate an attack on the site, producing a histogram for the at least one parameter of network traffic to characterize the attack by comparing the histogram to at least one historical histogram for that parameter, and filtering out traffic based on characterizing the traffic, which the gateway deems to be part of an attack.

Claims 33 and 34

The examiner contends that Appellant's arguments directed to "communicating statistics collected in the gateway to a control center." are not persuasive. Botros does not disclose this feature by disclosure of "a log and a database see Fig. 2 item 12 & 102" for the reasons of record.

Botros also does not disclose "a dedicated link to the control center via a hardened network" by: "... Fig. 1 & Fig. 2, where the direction of flow is unidirectional thus indicative of a dedicated network. And additionally, Botros discloses buses to interface with networks and storage see Fig. 15."

There is no teaching in Botros that correspond to a dedicated network between the gateway and control center and such feature is simply not met by a bus. Moreover, in Figs. 1 and 2 of Botros, they does not exist buses or networks, but mere generalizations of cooperation between the depicted elements.

Claims 37

The examiner has indicated allowance of claims 37-40.

For these reasons, and the reasons stated in the Appeal Brief, Applicant submits that the final rejection should be reversed.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 3/28/07

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906